REMARKS

Reconsideration of the present application, as amended, is respectfully requested. Claims 1-4 and 6-29 of the present application are currently pending. Claims 1, 6, 8, 9, 14, 17, 18, 22, 23, and 25-29 have been amended.

Applicant appreciates the opportunity to discuss the Examiner's rejection with the Examiner during the phone interview held on March 8, 2005.

Claim Objection

Claim 22 was objected to because of an informality. The claim was amended and is believed to overcome the objection.

Claim Rejections – 35 USC § 103

The Examiner rejected claims 1-4 and 6-29 under 35 USC § 103(a) as being unpatentable over US Patent 6,678,731 by Howard et al. (Howard) in view of US Patent 6,590,588 by Lincke et al. (Lincke). All of the independent claims have been amended to better reflect the invention. The amendments were not necessitated by the prior art or any other requirement of patentability, as discussed during the afore-mentioned interview. In light of the amendment, the Examiner's rejections have become moot. Nonetheless, the following remarks regarding the Examiner's rejections and the amended claims may be helpful to expedite prosecution.

Applicant's invention relates to a method of using a mobile communications device to access an on-line service provided by a network server, and more specifically, a method of enabling a proxy server to provide value-added services to a mobile device accessing a network server. The mobile device establishes one connection with a proxy server and a second, secure end-to-end connection with the network server, which contains the hypermedia information related to the on-line service. Typically, in prior art systems, if additional information is needed by the network server, a proxy server would not be able to

access communications on a secure connection between the mobile device and the network server, because the connection is secure and prevents any such access. Therefore, the proxy server would not be able to supply the value-added services' information. Applicant's invention overcomes these problems by also having an additional connection between the mobile device and the proxy server, thus permitting a request for additional information to be communicated from the network server to the mobile device, via the secure connection, from which, the mobile relays the request to the proxy server, which then can process the request and supply the additional information required, either to the mobile device, which then relays it back to the network server, or directly from the proxy server to the network server. In the applicant's invention the secure connection is not compromised and the proxy server has the ability to provide the required additional information, which would otherwise need to reside on the mobile devices' extremely limited memory. Applicant's invention also reduces the demands on the mobile devices' limited bandwidth and processing power, by allowing the proxy server to perform the requested functions on behalf of the mobile device, without compromising the secure connection.

Howard, in contrast, teaches a hard-wired system containing a client, a proxy server, and a network server, in which, there is a secure connection between the client and the proxy server. The proxy server is used to generate an authentication ticket, which can then permit the client to access various network servers. The proxy server also is used to distribute client information to network servers for various purposes, including promotional activities. The Howard system is designed to collect client data, process it, and distribute it to many network or affiliate servers, as well as, permitting the client to access many network servers simultaneously. See col.1, lines 24-35, and col.3, line 59 to col.4, line 2. Therefore, the client server in Howard needs to have high bandwidth, large memory, and a powerful processor. In order for the proxy server to collect data on the client, the client cannot have a secure connection with the network server because that would interfere with the proxy server's ability to collect such data. Therefore, the secure connection in Howard is **between the proxy server and the client**, and **not** between the network server and the client or mobile device.

Further, the Howard system is designed to produce an authentication ticket, which the client can use to access network servers. In Howard, the authentication ticket is generated by the proxy server, and used only for the purpose of accessing network servers. In contrast, the claimed invention requires "accessing a proxy server based service in order to obtain information required by the network server in order to process a request to the on-line service." Howard does not teach "a proxy server based service", nor that the network server generate a request to the proxy server, which is required for the on-line service. In contrast, Howard teaches that the proxy server generate an authentication ticket, which is then distributed to the network servers. There is no teaching that the network servers generate a request required for an on-line service.

Lincke teaches that prior art systems, such as that taught by Howard, are simply not compatible with mobile devices, unless the system includes the critical elements of Lincke's invention. See col.2, lines 53-64, and col.3, lines 6-23. Lincke makes use of a sensory cue, which identifies to the user, the data communication characteristics of the user request, so as to help the user decide whether or not they wish to initiate such a request. Lincke teaches that with a sensory cue, the user can avoid data downloads to the mobile device that would be prohibitively expensive and time consuming.

According to MPEP 706.02(j), a proper 35 USC 103 rejection requires three criteria, as described below:

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). See MPEP § 2143 - § 2143.03 for decisions pertinent to each of these criteria.

Howard fails to teach or suggest **all** the recited claimed elements. The claimed invention, both as amended and as previously presented, requires a secure connection between the mobile device and the network server. Applicant contends that neither Howard nor Lincke teach this element. Examiner has expressed, in the phone interview on 3/8/05, an interpretation of the claim limitation that a "secure connection", as recited in the claims, reads on an exchange of confidential information as exhibited in an authentication ticket described in Howard. Applicant asserts that a secure connection is not the same as the mere exchange of confidential information during authentication. A secure connection is defined in the art to be a connection that prevents or makes it more difficult for others to access the information conveyed across that connection. Although it may be reasonable to expect that confidential information would be kept secure, there are many different ways to secure such information without establishing a secure **connection** between the client and the network server.

Howard **actually teaches away** from the Examiner's interpretation by forming a secure connection between the client and the proxy server, which allows the proxy server to create an authentication ticket, containing confidential data. This authentication ticket and data is then widely distributed among many network servers, for many different purposes include sales and promotion. Howard specifically teaches securing the data at the client – proxy level, and provides no indication that the Howard system ever intended to create a secure connection at the client – network level. In Howard a secure connection at the client – network level would prevent the proxy server from extracting data from the interaction between the client and the network server, and interfere with the further processing and distribution of such data.

The claims have been amended to better reflect the invention. Some of the amended claims contain the limitation that requires the secure connection between

the mobile device and the network server to be established by tunneling through the proxy server. Neither Howard nor Lincke contain this limitation. Some of the amended claims also contain the limitation that the secure connection between the mobile device and the network server be encrypted. Neither Howard nor Lincke contain this limitation. Further, some of the amended claims contain the limitation that requires the secure connection between the mobile device and the network server to be established by bypassing the proxy server. Neither Howard nor Lincke contain this limitation. In addition, some of the amended claims contain the limitation that requires the secure connection between the mobile device and the network server to be established by encryption and tunneling through the proxy server. Neither Howard nor Lincke contain this limitation. Also, some of the amended claims contain the limitation that requires the secure connection between the mobile device and the network server to be established by encryption and bypassing the proxy server. Neither Howard nor Lincke contain this limitation.

The second criteria required for an obviousness rejection requires that there must be a **reasonable expectation of success**. The Examiner has correctly identified that Howard does not specifically include a mobile device as a client. Lincke teaches away from using mobile devices with a hard-wired system. Although, Lincke anticipates using mobile devices with a system, such as Howard's, it is only with the stipulation of using Lincke's sensory cue system, otherwise Lincke concludes that there would be no success. The expectation of success must be specifically identified with the combination being claimed and not with some other unclaimed combination contained within the cited references. In the instant case, the combination formed in the rejections are based on the presumption that a subset of the Lincke system, that excludes its critical element, would be combinable with Howard, but Lincke specifically teaches that such a subset would not be combinable. One of ordinary skill in the art, having Lincke and Howard's teaching, would have been advised not to combine Howard with

Lincke, due to an expressed expectation of failure within the Lincke reference itself. Applicant's claimed invention overcomes the concerns and problems expressed in Lincke by forming a secure connection between the mobile device and the network server, while also forming a connection between the proxy server and the mobile device, which is neither taught nor anticipated in either reference, alone or in combination.
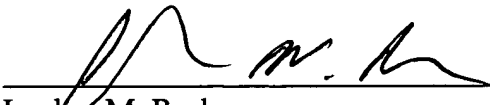
In conclusion, the claims, as amended, are asserted to overcome the Examiner's rejections and the claims are believed to be in condition for allowance. Applicants respectfully request reconsideration of this application as amended.

If there are any additional charges, please charge Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 3/16 , 2005

Jordan M. Becker
Reg. No. 39,602

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026
(408) 720-8300